Privacy Impact Assessment Update
for the

Science & Technology Analytic Tracking System (STATS)

DHS/S&T/PIA-032(a)

December 18, 2019

Contact Point
Ashley Stephenson
Finance and Budget Division
Science and Technology Directorate
(202) 254-5352

Reviewing Official
Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

The Department of Homeland Security (DHS) Science and Technology Directorate (S&T) Finance and Budget Division (FBD) operates the Science and Technology Analytical Tracking System (STATS), which supports financial, procurement, and acquisition management. As noted in the original STATS Privacy Impact Assessment (PIA), the system was designed to be upgraded to perform a human resources role. STATS will now collect, maintain, use, and transmit personally identifiable information (PII) of federal and contractor employees to perform human resources responsibilities. Information to be collected includes biographic data typically found in an employment record system as well as any associated human resources functions. This PIA update evaluates the privacy risks and mitigations associated with this new collection, maintenance, use, and transmission of PII.

Overview

The Department of Homeland Security (DHS) Science and Technology Directorate (S&T) deployed the Science and Technology Analytical Tracking System (STATS) in 2018 to support S&T financial, procurement, and acquisition management as performed by the S&T Finance and Budget Division (FBD).[1] FBD uses STATS to manage, track, and report on the full budget life cycle, including commitments (procurement requisition activity and workflow), obligations (awards, travel, and purchase card activities), and expenditures (all payment transactions), of the various projects and programs engaged in by S&T. It also includes a project tracker, electronic procurement request workflow tool, staff management tools, workforce management tools, data analytics, and a document repository.

STATS will now incorporate specific human resources (HR) functions that are currently being performed through the S&T Staff Management System (SMS).[2] These expanded capabilities require the collection, use, maintenance, and transmission of personally identifiable information (PII) of S&T personnel for HR functions. These upgrades not only incorporate the SMS human resources function, but also augment capabilities used for facilities management. Additional users of STATS will include the S&T Human Capital Office; the S&T Security, Preparedness, and Continuity Office (SPCO); and S&T Facilities Management personnel.

Reason for the PIA Update

S&T is publishing this PIA update to document STATS' new HR function. Previous functions are documented in the original PIA. Given its developmental history and intended use as a budget and project management tool, when STATS was implemented in 2018 only a small amount of PII was housed in the system. STATS was, however, specifically designed as a scalable

[1] For the original PIA, please *see* DHS/S&T/PIA-032 S&T Analytical Tracking System (STATS), *available at* https://www.dhs.gov/privacy.
[2] *See* DHS/S&T/PIA-002 S&T Staff Management System (retired), *available at* https://www.dhs.gov/privacy.

information technology system. Planned upgrades to include HR functions were envisioned from the outset. To that end, S&T is transferring its HR functionality from SMS to STATS. Thereafter, SMS is scheduled to be decommissioned.

The upgrades allow for the management of HR activities at S&T while minimizing the number of disparate information technology systems processing PII being maintained by S&T. These functionalities include the on-boarding and off-boarding process, results of suitability assessments, tracking the office assignment of S&T personnel, managing personnel and position data, and other associated HR functions. In addition, STATS includes the addition of facilities management users.

As part of the STATS update, four modules are being added to implement the new HR functionality. The Positions Module enables users to create, maintain, and view employment positions in the system that can be assigned to specific personnel. The Facilities Module enables users to create, maintain, and view facility information including specific buildings, floors, seats, rooms, and room keys data. The Federal Personnel Module enables users to create, maintain, and view information related to federal employees for personnel management purposes. The Contractor Suitability Module enables users to create, maintain, and view contract employee information related to the contractor suitability process.

This PIA update is necessary to assess the privacy risks and mitigations attendant to STATS' new functionalities that include the collection, use, maintenance, and transmittal of PII associated with HR requirements. The additional data elements, not previously covered by the original STATS PIA, that are being added to STATS are detailed in the *Characterization of the Information* section of this PIA update. Further updates to this PIA will be made when new STATS functionalities and capabilities require new or revised privacy assessments.

Privacy Impact Analysis

The authority for accessing, collecting, using, and maintaining PII, including Social Security numbers (SSN), and other information on S&T personnel is:

> The Homeland Security Act of 2002, as amended, 6 U.S.C. § 341(a)(3); 44 U.S.C. § 3101 "Records Management by Agency Heads"; 5 U.S.C. Part III, "Employees"; Executive Order 9397 (November 22, 1943), *as amended by* Executive Order 13478 (November 18, 2008).

Previously, STATS did not require system of records notice (SORN) coverage because STATS did not originally retrieve records of individuals using an individual identifier. The introduction of HR functions means that STATS will be used to search and retrieve PII using an individual identifier. The following SORNs apply to STATS accessing, collecting, using, and maintaining PII and other information in connection with its upgraded HR functions:

OPM/GOVT-1 *General Personnel Records,*[3] which covers the general authority of the Federal Government to collect various information on both federal and contract employees for purposes of creating and maintaining an Official Personnel Folder (for federal employees) and general HR functions;

GSA/GOVT-3 Travel Charge Card Program,[4] which covers the information collected to track the issuance of purchase and travel cards within STATS;

DHS/ALL-004 *General Information Technology Access Account Records System (GITAARS),*[5] which covers the information used to grant S&T personnel employees access to STATS;

DHS/ALL-014 *Department of Homeland Security Personnel Contact Information,*[6] which covers the information maintained for emergency contact information and other contact information of S&T personnel;

DHS/ALL-023 *Department of Homeland Security Personnel Security Management,*[7] which covers the information used by DHS for determining employee and contractor suitability; and

DHS/ALL-032 *Official Passport Application and Maintenance Records,*[8] which covers the information necessary for DHS to issue personnel Official United States Passports to be used when traveling abroad on official U.S. Government business.

As part of the STATS update, a System Security Plan was last updated on November 7, 2019. Additionally, S&T determined that the appropriate records retention and destruction schedules of the additional information collected, used, maintained, and transmitted by STATS due to its new HR capabilities are governed by the National Archives and Records Administration's (NARA) General Records Schedule 2.2, *Employee Management Records*.

Characterization of the Information

The new STATS human resources data fields maintain the below information. STATS users collect data: (1) directly from the individuals;[9] (2) through documentation prepared by the

[3] OPM/GOVT-1 General Personnel Records, 77 FR 73694 (December 11, 2012).
[4] GSA/GOVT-3 Travel Charge Card Program, 78 FR 20108 (April 3, 2013).
[5] DHS/ALL-004 General Information Technology Access Account Records System (GITAARS), 77 FR 70792 (November 27, 2012).
[6] DHS/ALL-014 Department of Homeland Security Personnel Contact Information, 83 FR 11780 (March 16, 2018).
[7] DHS/ALL-023 Department of Homeland Security Personnel Security Management, 75 FR 8088 (February 23, 2010).
[8] DHS/ALL-032 Official Passport Application and Maintenance Records, 76 FR 8755 (February 15, 2011).
[9] Federal employees are contacted by STATS users when they are being onboarded and assigned to a representative. Contractors typically provide their information to their company, which then provides the information to an S&T Contract Officer Representative (COR) and the information is entered into STATS.

individual; and (3) maintained in the Integrated Security Management System (ISMS)[10] about suitability determinations once the individual has been granted suitability.

- *Personnel Data* includes name, gender, place/date of birth, citizenship status, SSN, business phone number, business email address, building location, DHS organization structure code, emergency contact information (first name, last name, relationship, primary and secondary phone numbers – for federal employees only), salary (federal only), planned retirement date (federal only), and travel and purchase cards information (federal only).
- *Position Data* includes position title, position risk level (designates risks within a contract as either low, moderate, or high, and likewise indicates the level of access to National Security Information if necessary), security clearance level, and pay grade and step level (federal only).
- *Contract data* includes date of submission, DHS organization, type of request, exit request reason, Contract Officer (CO) name, CO business phone number, CO business email address, Contract Officer Representative (COR)/federal point of contact (POC) last name, COR/POC business phone number, COR/POC business email address, prime contractor, prime contract number, task order number, whether a PIV is required, and SSN.

The sources of the new information STATS collects to support the HR capabilities and functions and how that information is collected are outlined below.

- *Information Transfer from SMS.* All active S&T personnel records (both federal employees and contractors) are transferred from the legacy SMS environment to STATS in a one-time transfer. As individuals leave the employment of S&T or are no longer S&T contractor workforce members, they will be flagged as inactive in STATS. This will ensure that no further processing will be possible for those individuals. Flagged inactive records will remain in STATS for historical purposes in adherence with the approved NARA records schedule.
- *New S&T Federal Employees.* The Human Capital Office (HCO), as part of the established hiring and on-boarding of new S&T federal employees, collects information from the individual for establishing the individual's Official Personnel File. Federal employee data entered into STATS is also obtained from the individual's employment application and information accessed by HCO staff in ISMS. The relevant data elements from those records are inputted into STATS by HCO staff after the federal employee has cleared the suitability assessment.

[10] *See* DHS/ALL/PIA-038 Integrated Security Management System (ISMS), *available at* https://www.dhs.gov/privacy.

- *New S&T Contractor Employees*. Information on contractor employees is collected by their employer and provided to the S&T COR for that contract, who then enters that information into STATS. For suitability determinations, the contractor fills out DHS Form 11000-25 (*Contractor Fitness/Security Screening Request* Form), which is then reviewed by S&T Security, Preparedness, and Continuity Office (SPCO) for accuracy. This form is used to request that the DHS Office of the Chief Security Officer (OCSO), Personnel Security Division perform the appropriate fitness screening on contract employees.

The new information collected, used, disseminated, and maintained by the upgraded functionality of STATS does not originate from commercial sources or publicly available data. Rather, the information collected by STATS is taken from the existing SMS, ISMS, or directly from the individual or individual's corporate employer, during the individual's initial on-boarding process or throughout his or her employment period.

Privacy Risk: STATS data may be inaccurate or incomplete.

Mitigation: This risk is not fully mitigated as much of the data in STATS is manually entered. However, S&T has taken several steps to provide mitigating factors. S&T receives the information directly from the individual when possible, either through a copy of an HR or hiring and on-boarding document or through a STATS user acting as the individual's representative. S&T has taken the necessary DHS policy requirements to transfer current S&T personnel information from the existing SMS in a one-time transfer.[11] Additionally, STATS uses suitability information from ISMS, the Department's authoritative personnel security database. This information is updated manually by STATS users as there is no direct interface with ISMS. STATS users are trained to verify the information they receive by confirming it directly with the individual or based on the documentation provided and resolve any discrepancies as necessary.

Privacy Risk: There is a risk that data in STATS is outdated because the data is manually refreshed.

Mitigation: This risk is partially mitigated. Federal personnel are directed[12] to update the HCO of any changes and or updates to their biographic information if the updated information would trigger updates to other STATS data fields. Contract personnel are directed to similarly update their COR with any changes that occur.

[11] The S&T Office of the Chief Information Officer (OCIO) monitors the development and deployment of new functionalities for STATS. This includes the transfer of any data from SMS to STATS. OCIO follows the DHS requirements under the "DHS 4300A Sensitive Systems Handbook," *available at* https://www.dhs.gov/sites/default/files/publications/4300A%20Sensitive-Systems-Handbook-v12_0-508Cs.pdf.

[12] *See* DHS Management Directive No. 008-04 (Sept. 19, 2006), *available at* https://www.dhs.gov/sites/default/files/publications/mgmt/disaster-management/mgmt-dir_008-04-personnel-accountability-directive_revision-00.pdf.

Uses of the Information

In its expanded capabilities, STATS is designed as a human resources management tool in addition to its original role as a budget, data repository, and process management tool. STATS will allow users to perform on-boarding activities, initiate contractor suitability assessment requests, assign personnel to physical workspaces, and perform off-boarding activities. STATS also allows users to generate demographic and position reports used for workforce planning, budgeting, and attrition monitoring. STATS will enable the tracking of both travel and purchase cards for federal employees as well as the issuance of official passports when necessary. As listed below, each user role is able to narrow datasets based on search parameters to produce various reports generated by STATS.

Finally, as STATS is specific to S&T, no other DHS components are assigned roles or responsibilities within the system.

Privacy Risk: Due to number of functions performed within STATS, individuals may have access to data for which they do not have a need to know.

Mitigation: This risk is mitigated because STATS uses role-based access control lists to ensure that only authorized users access specific information. All users of STATS fit into a hierarchy of authorized access (discussed more fully below) that delineates a user's access to specific data fields. Thus, for example, only select users are permitted to view an entire SSN, thereby limiting the number of users able to modify that data field.

Authorized users log into STATS using their Personal Identity Verification (PIV) card and their personal identification number (PIN).[13] Obtaining a STATS user account requires an individual to submit a STATS User Account Request through the STATS Help Desk. Through the STATS User Account Request process, a user is assigned his or her specific role within the access hierarchy. The user's assigned role establishes the scope of access to the STATS database and the functionality and capability accessible to that user. These limits on scope and access are defined and restricted by STATS' role-based access controls.

STATS' role-based access controls provide assurances that its users may access only the specific functions, data, and modules (e.g., Position Module, Contractor Personnel Module, the Facilities Management Module, and Federal Personnel Module) required to perform their assigned duties. These role-based access controls are detailed below.

1. S&T HCO staff will

[13] A PIV card is a government-issued identification badge developed in response to Homeland Security Presidential Directive-12 (*available at* https://www.dhs.gov/homeland-security-presidential-directive-12). DHS federal employees and contractors are issued PIV cards and each PIV card is coded to permit or deny access to both government facilities and information technology systems. For additional information on PIV cards, *see* https://piv.idmanagement.gov/elements/.

   a. Create and maintain all federal and contractor personnel data associated with the new human resources capabilities of STATS;
   b. Have access to the STATS Position Module, Contractor Personnel Module, the Facilities Management Module, and Federal Personnel Module; and
   c. View/update all personnel information. All personnel within this role are federal employees that are required to manage records for S&T's human resources functions.

2. S&T contract Points of Contact (POC)/CORs will
   a. Maintain all contractor personnel data for their assigned contracts only;
   b. Have access to only the Contractor Personnel Module; and
   c. View/update contractor personnel information. This role is required as the POCs/CORs are responsible for submitting contractor employees for a suitability determination to the S&T Security, Preparedness, and Continuity Office. All personnel within this role are federal employees that are required to manage records for contract functionality and manage the staffing of contracts for which they are responsible.
3. S&T SPCO will
   a. Review and maintain contractor data as necessary in preparing DHS Form 11000-25 (*Contractor Fitness/Security Screening Request* Form) for the DHS OCSO for suitability assessment. S&T HCO and SPCO staff handle this document securely pursuant to DHS Acceptable Use standards and the form history will be maintained in STATS;
   b. Have access to only the Contractor Personnel Module;
   c. View/update contractor personnel information. All personnel within this role are federal employees that are required to manage contractor records for the submission of suitability determinations to DHS OCSO.
4. S&T Facilities Management will
   a. Establish and maintain all data related to physical office assignments. Additionally, this role will track the issuance of purchase and travel cards within STATS;
   b. Have access to only the Facilities Management Module; and
   c. Not need to view/update all PII, such as SSNs, as it is not required. Users may access limited information on individuals for work space assignments. S&T

Facilities Management personnel need access to assign and manage data associated with the physical placement of federal and contract employees.

Mitigation of Risks relating to Collection, Use, and Storage of SSNs

The new human resources functionalities and capabilities of STATS require the collection, use, and storage of SSNs. Consistent with the DHS SSN Reduction Initiative,[14] the following safeguards are deployed by STATS:

1. SSNs are encrypted at rest in the STATS database;
2. Access to SSNs is role-based and SSNs are omitted from view for users not requiring access;
3. SSNs are used by STATS only as a data element in DHS Form 11000-25 processing and for duplication verification; and
4. SSNs are not used as a unique identifier in the STATS database. Searches may be performed using the last four digits of a SSN; however, the last four digits of a SSN are not a unique personal identifier.[15]

Other Mitigation of Unauthorized Access Risks

In addition to safeguards regarding physical access to DHS facilities, the unauthorized access to DHS network and information systems is also protected through boundary protection devices (e.g., firewalls). Intrusion detection capabilities are installed at the network level to detect system and network anomalies that may impact STATS security. Encryption is used to securely transmit all data between the user’s web browser and STATS servers. This mitigates the risk of data compromise while in transit. PII is encrypted at rest in the database to mitigate the risk of unauthorized data access.[16] Data fields encrypted at rest in the database include SSNs and dates of birth.

When a contractor suitability determination is necessary, STATS generates the DHS Form 11000-25 in portable document format (PDF) which includes a full SSN. This PDF is then sent via encrypted email to DHS OCSO security personnel.

Privacy Risk: Reports generated by STATS may contain data that a user may not be authorized to view or receive.

[14] *See* DHS Instruction No. 047-01-010, *Social Security Number Collection and Use Reduction* (June 18, 2019), *available at* https://www.dhs.gov/publication/privacy-policy-instruction-047-01-010-ssn-collection-and-use-reduction.

[15] There are only 10,000 unique combinations available in any four-digit number sequence. Additional PII is necessary to make the connection between the two data elements to confirm identity.

[16] Encryption at rest is provided via FIPS 140-2 256 bit encryption. Encryption in transit is provided by HTTPS TLS 1.1/1.2 256 bit encryption. Additionally, the S&T STATS database server is protected by multiple firewall layers (web tier firewall, application tier firewall, database server firewall) and further protected by SQL Server authentication.

Mitigation: This risk is mitigated through management, operational, and technical controls, including role-based access controls. Authorized STATS users may generate and print reports of demographic and position data used in workforce planning, budgeting, attrition monitoring, and general human resources and facilities management. STATS-generated reports are not customizable by an individual user. Rather, they are standard reports approved as to form and content by the system owner as part of a development cycle based on documented requirements for each user role. Any change to a standard report must be made using the same development cycle and system owner approval process.

STATS-generated reports limit access to PII based upon the access hierarchy each user is assigned to. In this way, the user may generate reports containing the data specific to the needs of his or her duties. Encrypted PII (SSNs and dates of birth) is not permitted in these reports. Users may only view and print their approved reports. Users do not have the ability to change or access data not displayed in their approved report(s).

Notice

The new human resources functionalities and capabilities use data drawn from either the existing SMS, ISMS, or directly from the newly on-boarded individuals or prospective contractor staff. In general, except for this updated PIA and the notice provisions contained in the applicable SORNs, there is no specific notice to individuals that their biographic information will be collected, used, maintained, and transmitted in STATS.

Privacy Risk: Individuals whose information is maintained in STATS do not have notice of how their information will be used.

Mitigation: This risk is partially mitigated by publication of this PIA update and the SORNs referenced above. Although there is no specific notice at the time of collection, S&T personnel (and their emergency contacts – generally family members) may reasonably expect that biographic information may be collected, maintained, and used by S&T for administrative, management, and human resources functions. Additionally, personnel are notified that specific biographic information is required for obtaining a PIV card, and to successfully complete the on-boarding and suitability processes.

Data Retention

NARA General Records Schedule (GRS) 2.2, Employee Management Records, outlines the retention requirements for the human resources data and the data stored within STATS. STATS records are destroyed when three years old, but longer retention is authorized if required for business use. Upon leaving employment with S&T, STATS users manually flag the individual's specific personnel record as inactive. This change in status from active to inactive is made during the individual's off-boarding process. Inactive STATS records are maintained for historical purposes as authorized under GRS 2.2. Other than for this use in historical reports, STATS does not use, or permit changes to be made to, records flagged as inactive. STATS administrators conduct routine reviews and audits to ensure that data is properly deleted.

Active personnel records in SMS will be transferred to STATS and SMS will be decommissioned. Once decommissioned, inactive personnel records in SMS will be retained in accordance with applicable GRS 2.2 and applicable destruction requirements.

This retention also aids the S&T HCO in responding to personnel inquiries from other government agencies performing new-hire employment verification and background investigations on previously employed S&T personnel.

Privacy Risk: STATS data and STATS-generated reports will be retained longer than necessary or inconsistently with applicable records retention schedule(s).

Mitigation: This risk is not fully mitigated. STATS data and STATS-generated reports may have historical use or value beyond their initial creation. Therefore, the business use of the data is likely to continue for several years beyond its creation. Until the development of automated processes within STATS to assure timely data disposition, manual processes currently in place will ensure all applicable records retention schedules are implemented. These manual processes include an inherent human error factor in determining whether records are subject to disposition under an applicable retention schedule. S&T will implement audit procedures to ensure appropriate manual data destruction is undertaken.

Information Sharing

STATS maintains existing practices as it relates to sharing and disclosure of data collected for capabilities other than human resources (e.g., project tracking, electronic procurement workflow tool, document repository). The human resources modules in STATS may share information outside of DHS in accordance with the routine uses listed in the OPM/GOVT-1 and other applicable SORNs listed above. The upgraded STATS human resources functionality has additional privacy risks with respect to the sharing and disclosure of the data due to the sensitive nature of the PII.

Privacy Risks: Individuals authorized to access STATS will conduct unauthorized activities, such as extracting and sharing information with unauthorized recipients.

Mitigation: This risk is partially mitigated. Authorized STATS users are required to sign the DHS Rules of Behavior, a Non-Disclosure Agreement, and obtain their supervisor’s approval to gain access to STATS. A privacy policy and security statement appear on each STATS login screen reminding the user of the proper uses of the system. Punishments for failure to comply with these Rules of Behavior include a verbal or written warning, removal of system access, reassignment to other duties, criminal prosecution, civil liability, and/or termination of employment.

STATS audits data based on user requirements. Auditing tools track any modifications of specified data fields as well as any deletion of data. In addition, the audit tools track common attributes such as user identification, the nature of the data change, and when the change took place.

As previously described, STATS users are placed into the access hierarchy based on the user's assigned duties. The Chief of Staff of S&T has instituted policies and procedures to approve user access to personnel information. The users of this system who have access to personnel information are S&T Directors/Deputies, S&T SPCO personnel, S&T HCO staff, S&T Facilities Management staff, and S&T Chief Financial Office staff. These user access roles limit the PII able to be viewed by the user according to their assigned duties.

Redress

Not all the HR information in STATS is entered using an automated process. Data fields are manually inputted by HCO staff. Because of this manual process, data entry errors are possible. As discussed above, S&T personnel are required to maintain up to date contact information. If errors exist, they will generally be noticed in STATS-generated documents. There are specific redress procedures to follow depending on whether that individual is a federal employee or a contract employee. S&T contractor employees should contact either their corporate Facility Security Officer or the COR for their contract to request a specific update/amendment. Federal employees of S&T should contact the HCO to request a specific update/amendment. All employees are provided with contact information of the HCO staff during their on-boarding process and additional information can be found on the S&T intranet.

Additionally, individuals may request access to information about them that may have been retained in STATS pursuant to the applicable provisions of the Freedom of Information Act (FOIA) or Privacy Act (PA). An individual may submit a FOIA or PA request to S&T by mail to the S&T FOIA Coordinator, Mail Stop: 0210, Department of Homeland Security, 245 Murray Lane SW, Washington, D.C. 20528.

Auditing and Accountability

Audit and accountability policies and procedures exist to ensure that risks, vulnerabilities, and threats are properly identified, analyzed, documented, and adequately managed. STATS adheres to the DHS security access control policies contained in DHS Sensitive Systems Policy Handbook 4300A. That document addresses the purpose, scope, roles, responsibilities, management commitment, coordination among DHS entities, and compliance.[17] The system is scanned for vulnerabilities twice a week, and a Security Information and Event Management tool is used to continuously monitor audit logs.

[17] *See* DHS Sensitive Systems Policy Handbook 4300A, *available at* https://www.dhs.gov/sites/default/files/publications/4300A%20Sensitive-Systems-Handbook-v12_0-508Cs.pdf.

The policies and procedures encompass user activity during the operational and maintenance phase of the system. Audit trails for a variety of system-related events and activities are logged to allow the system administrator and system ISSO to check for associated security issues. The items recorded provide an accurate representation of the actions taking place, the user responsible for initiating the action, and the date and time.

The level of user activity logging is tailored to the needs of the system, with specific focus upon the Program Management and Reviewer users, who have access to sensitive information. Each time an attempt is made to log in to the system with an invalid username, the system logs the username, date/time, and IP address of the computer trying to gain access. Additionally, after three unsuccessful access attempts a user's access is locked until the situation can be reviewed and remediated by an appropriate system administrator. These logs are reviewed weekly by the ISSO to determine the appropriate course of action. The audit facility logs insert, update, and delete operations to the system log file and to the database audit tables including identification of: DHSNET username (associated with user session), date/time, database table, database operation performed, and specific content modified.

Privacy training is provided during STATS user training, prior to providing access to the system. All S&T staff receive training regarding appropriate use and management of personal information. All new S&T workforce members receive introductory privacy, security, and records management training as part of their onboarding.

Responsible Official

Carol Cribbs
Principal Director
Office of Enterprise Services
Science and Technology Directorate

Maria Petrakis
Privacy Officer
Science and Technology Directorate

Approval Signature

Original, signed copy on file with the DHS Privacy Office.

____

Jonathan R. Cantor
Acting Chief Privacy Officer
Department of Homeland Security